Department of Health
Policy/Procedure

Title:	Information Technology Security	Number: 10.002
References	DOH Policy 14.003	
Contact:	Office of Information Resource Management, Data Resource Management , Security Administrator	
Effective Date:	December 23, 1998	
Supersedes:	Policy 10.002 dated September 1, 1994	
Approved:	Signed by Mary C. Selecky	
	Secretary, Department of Health	

Purpose:

This policy defines the framework of security administration for all divisions of the Department of Health (DOH).

Information, regardless of its source, is a valuable asset to the Department of Health. Its accuracy and confidentiality are essential to the mission of the department to maintain the public's trust. It must be protected from inadvertent or intentional misuse, disclosure, fraud, and loss.

Controls minimize the vulnerability of information and provide the necessary security to protect it. The Security Administrator for the Department of Health establishes and reviews security controls for the agency.

Definitions:

Information Technology (IT) is defined as the equipment, software, services, and products used in storing, processing, transmitting, and displaying all forms of information. Information technology includes data processing, office automation, multimedia, hard copy, and telecommunications.

Userid is a unique code that identifies the user of a computer system. Also called loginid.

Signon is the process of entering userid and password to activate software or operating system capabilities.

Software is a computer program that has been compiled or otherwise made ready to "run" or "execute". Without software, computers are useless.

A computer program is an organized list of instructions that, when executed, causes the computer to behave in a predetermined manner.

External-origin software and data originate from outside the DOH network, including files received via e-mail, Internet, file transfers, diskettes, CDs, or any other source.

ASCII files, as they relate to virus control, are generally data files and are not program-specific. This is different from **binary files**, such as Microsoft Word documents (e.g. filename.doc), Excel spreadsheets (e.g. filename.xls), or executable programs (e.g. filename.exe or filename.dll). DaVinci Mail identifies ASCII attachments as "[Text]".

Privileged rights are special access rights that allow relatively unrestricted access to a system and are not normally granted to the casual user.

Policy:

1. The Department of Health owns the systems and data residing on agency owned and leased computing equipment; or equipment for which the agency is a trustee (e.g. federally owned/sponsored equipment).

2. Security in the DOH will be promoted using standards and guidelines developed in cooperation with all of the divisions, maintained centrally, and applying to the agency as a whole.

3. External-origin software will not be installed on agency laptops, workstations and networks unless approved by division management and Campus Technical Support Teams. The Security Administrator will provide risk assessment, upon request, to minimize adverse impact to DOH networks from untested software.

4. Virus checks, using approved virus detection software, must be performed on all external-origin files (except ASCII files) before or immediately after they are saved or installed on agency laptops, workstations and networks.

5. Userid and password must be manually entered. Signon scripts (e.g. userid and password imbedded in a .BAT script) to log onto the network or application are not allowed unless approved by division management and OIRM.

6. Users must choose unique passwords and keep them secret. Passwords are to be used only by the person assigned to the userid. Passwords, on all systems, must be changed every 60 days or less. Use of hard to guess passwords, e.g. using random numbers and characters, is encouraged. Passwords for userids with privileged rights must be changed every 30 days or less.

7. Userids are not meant to be shared. Users are accountable for all activity associated with their own userid. Signon access can be considered the same as signature authority.

8. When it is necessary for someone to access another person's electronic mail, electronic calendar, or LAN work areas, rights will be approved by the person whose area is to be accessed and set up by the Campus Technical Support Team according to features available within the software.

9. Unique userids are maintained for all users of DOH computing resources. This includes all permanent, temporary, contract and project employees, contractors, and external users. Userids can only be shared under special provisions approved by division management, Campus Technical Support Teams and the Security Administrator. In all cases, one person will be responsible for the userid and for maintenance of the password. Unique userids are required for all state and local agency personnel who have a need to access the DOH systems as described in RCW 43.105.

10. Auditing provides the monitoring necessary to catch failures in the authentication system and to produce documentation that all is well. Accounting processes that produce log files will be activated in order to audit authenticated access to the LAN and monitor user activity, where division management and Campus Technical Support Teams designate the cost is warranted. The Security Administrator will assist with this analysis. Accounting processes on all dial-in systems must remain activated.

11. Personnel terminating employment and contractors terminating contractual activity requiring access to DOH computing systems will have their systems access disabled on or before their last working day. Personnel beginning employment with DOH, beginning contractual activity requiring access to DOH computing systems, or transferring within DOH will be given access at their new office no sooner than their first working day in their new position.

12. The Security Administrator will coordinate security with System Administrators (UNIX, NT, etc.), DataBase Administrators, Network Administrators, , Campus Technical Support Teams, applications systems analysts, and division management

13. Access to network and operating system by vendors, contractors, and visitors will be granted on an as-needed basis only in the same manner as all other requests for access. Privileged rights will not be granted unless approved by program management and OIRM. Vendor access to a new system must be terminated prior to processing production data and allowed for problem resolution on an as-needed basis only.

14. All production data and software files must be backed up weekly or more often as data activity dictates. Backup copies of production files must be stored in a secure off-site facility and rotated regularly. A full restore of backup data must be tested semi-annually; more often for sensitive data. Backups kept on-site must be secured away from workstations and consoles commensurate with the level of confidentiality and sensitivity of the data.

15. All files/programs/data must be removed from the computer equipment before leaving the agency. For computers, this means completely over-writing the hard drive with a program that meets Department of Defense specifications (DoD 5220.22-M). It is not sufficient to simply erase all the data, or even reformat the hard drive. For machines that are inoperable, the hard drive should be physically destroyed. Portable storage mediums (e.g. floppy disks, backup tapes) should be degaussed or destroyed.

Procedures:

Responsibilities:	**Action:**
Assistant Secretary	• Responsible for data and access to that data which is managed by the division. • Set confidentiality criteria and rules for division managed data that may be distributed outside of the agency. • Ensure divisional compliance with security policies of the agency.
Security Administrator	• Coordinate security for the agency. • Set up access to mainframe systems. • Assist System Administrators, DataBase Administrators, Network Administrators and Campus Technical Support Teams with security-related design and implementation issues. • Review requests for exceptions to security policy, such as scripted logins or shared userids. • Assist technical staff and program management with computer emergencies or potential breaches of access. • Provide technical assistance to Assistant Secretaries in developing confidentiality criterial and rules for division-managed data that may be distributed outside of the Agency.

Security Administrator, System Administrator, DataBase Administrator, Network Administrator, , Campus Technical Support Teams	• Assign userids and startup passwords. • Reset passwords as requested by user. • Set user access rights according to business needs, agency standards, and industry best practices regarding security. This applies to network access, system resources and data on all systems. • Monitor access and notify Security Administrator of suspected security breaches. • Ensure that backups are performed as scheduled and stored securely, including offsite storage as provided. • Ensure that all data storage media no longer in service are free of confidential information.
Manager, Procurement and Distribution	• Coordinate with the appropriate technical support team to insure PCs being processed for surplus are cycled through the campus support team to insure data storage media is free of data.
Employee	• Notify supervisor and either the Campus Technical Support Team or the Security Administrator, of any suspected security breaches to the workstation, network, and facility. • Accept responsibility for all activity performed under their own personally assigned userid. • Scan all external-origin files for virus infection prior to loading or executing on any DOH workstation, laptop or network.